XIX Semana Olímpica de Matemática

Nível 2

Divisibilidade

Carlos Shine

O projeto da XIX Semana Olímpica de Matemática foi patrocinado por:

Divisibilidade

Carlos Shine

1 Alguns princípios básicos

- **Combinação linear**: se $d \mid a$ e $d \mid b$, então $d \mid ax + by$. Como consequência, temos o *teorema de Bézout*: $\{ax + by, x, y \in \mathbb{Z}\} = \{\mathrm{mdc}(a, b)x, x \in \mathbb{Z}\}$. Ou seja, o conjunto das combinações lineares de a e b é igual ao conjunto dos múltiplos de $\mathrm{mdc}(a, b)$.
- **Divisor $\leq$ múltiplo (ou o múltiplo é zero)**: se $d \mid a$ então $a = 0$ ou $|d| \leq |a|$. Isso é importante quando d e a são polinômios de várias variáveis, e você quer limitar as soluções.
- **Congruências em divisibilidade**: se $d \mid a - b$ então você pode trocar livremente a por b e vice-versa em divisibilidades, já que $a \equiv b \pmod{d}$.
- mdc **para cortar**: se $d \mid ab$ e $\mathrm{mdc}(a, d) = 1$, então $d \mid b$. Isso é útil para diminuir grau e usar divisor $\leq$ múltiplo.
- **Para calcular** mdc: se $d = \mathrm{mdc}(a, b)$ então $d \mid a$ e $d \mid b$. Note que a volta não vale.
- **I** $\heartsuit$ ± 1: fique esperto quando aparece algum número 1; isso deve ajudar no mdc.
- **Não consegui calcular o** mdc**, o que faço?** Se não se sabe sobre o mdc, pode valer a pena fazer $d = \mathrm{mdc}(a, b)$, $a = dx$ e $b = dy$ com $\mathrm{mdc}(x, y) = 1$.
- **Desigualdades automáticas**: se você perceber alguma relação de desigualdade do tipo $a > b$, pode valer a pena introduzir uma variável que reflita essa desigualdade; no nosso exemplo, seria $k = a - b$. Note que isso nos isenta de *lembrar que* $a > b$.

Exemplo:
(IMO 1992) Encontre todos os inteiros positivos a, b, c com $1 < a < b < c$ tais que $abc - 1$ é múltiplo de $(a - 1)(b - 1)(c - 1)$.

Resolução:
Vamos simplificar o divisor com uma mudança de variável. Sejam $x = a - 1$, $y = b - 1$ e $z = c - 1$. Assim queremos saber os inteiros positivos x, y, z tais que xyz divide $(x + 1)(y + 1)(z + 1) - 1 = xyz+xy+yz+zx+x+y+z$. Podemos ignorar o xyz no múltiplo, logo temos $xyz \mid xy+yz+zx+x+y+z$.

Produtos de três números inteiros positivos geralmente são maiores do que produtos de dois números inteiros positivos, então vamos usar a desigualdade divisor $\leq$ múltiplo:

$$xyz \leq xy + yz + zx + x + y + z < 6yz \implies x \leq 5.$$

Ter só cinco casos é bom, mas dá para fazer melhor: lembre que $0 < x < y < z \iff 1 \leq x \leq y - 1 \leq z - 2$. Com isso, tentado fazer aparecer yz em todas as contas,

$$xyz \leq xy+yz+zx+x+y+z \leq y(z-2)+yz+z(y-1)+x+y+z = 3yz+x-y \leq 3yz+y-1-y = 3yz-1 < 3yz,$$

logo $x < 3$, ou seja, $x = 1$ ou $x = 2$. Ficamos só com dois casos!

- $x = 1$: temos $yz \mid y + yz + z + 1 + y + z \iff yz \mid 2(y+z) + 1$ e mais uma desigualdade:
$$yz \le 2y + 2z + 1 \le 2(z-1) + 2z + 1 = 4z - 1 < 4z \implies y \le 3.$$
Logo $x = 1$, $y = 2$ e $2z \mid 2z + 5$, que é impossível pois $2z$ é par e $2z + 5$ é ímpar, ou $x = 1$, $y = 3$ e $3z \mid 2z + 7 \implies z \mid 7 \iff z = 7$ e verificamos que $3 \cdot 7 \mid 2 \cdot 7 + 7$, e $(x, y, z) = (1, 3, 7) \iff (a, b, c) = (2, 4, 8)$ é solução.

- $x = 2$: temos $2yz \mid 2y + yz + 2z + 2 + y + z \implies yz \mid 3y + 3z + 2$ (ignoramos o 2 para podermos cortar o yz). Com isso,
$$yz \le 3y + 3z + 2 \le 3(z-1) + 3z + 2 = 6z - 1 \implies y \le 5.$$
Além disso, $2 \mid yz + y + z \iff 2 \mid (y+1)(z+1) - 1$, o que quer dizer que y e z são ambos pares. Logo, como $2 = x < y \le 5$, $y = 4$ e o problema é equivalente a $8z \mid 7z + 14 \implies z \mid 7z + 14 \iff z \mid 14 \implies z = 14$. Testando, vemos que $8 \cdot 14 \mid 7 \cdot 14 + 14$, e $(x, y, z) = (2, 4, 14) \iff (a, b, c) = (3, 5, 15)$ é outra solução.

Assim, as únicas soluções são $(2, 4, 8)$ e $(3, 5, 15)$.

2 Equação do segundo grau

Às vezes não dá para fazer o grau do múltiplo ser menor do que o grau do divisor; nesse caso, você pode usar equações do segundo grau para gerar soluções. Os passos costumam ser os seguintes:

1. Transforme o problema em encontrar pares de inteiros positivos que satisfazem uma equação quadrática em uma delas. Em geral, diminuir o grau usando d divide ou congruências ajuda.
2. Considere uma solução mínima (soma mínima, menor variável mínima, etc).
3. Gere uma solução a partir dessa solução (usando soma e produto) e verifique que ou ela é maior ou igual à mínima ou tem algum cara negativo.
4. Encontre as soluções mínimas e gere, se houver, todas as outras.

Veja o seguinte exemplo:

Exemplo:
(IMO 2007) Sejam a e b inteiros positivos tais que $4ab - 1$ divide $(4a^2 - 1)^2$. Prove que $a = b$.

Resolução:
Como $1 \equiv 4ab \pmod{4ab-1}$, $(4a^2-1)^2 \equiv (4a^2 - 4ab)^2 \equiv 16a^2(a-b)^2 \pmod{4ab-1}$. Sendo $\mathrm{mdc}(4ab - 1, 16a^2) = 1$ (por quê?), $4ab - 1 \mid (a-b)^2$.

Suponha, por absurdo, que $a \neq b$. Então $k = \frac{(a-b)^2}{4ab-1}$ é um inteiro positivo. Essa última equação é equivalente a
$$a^2 - (4bk + 2b)a + b^2 + k = 0.$$

Considere uma solução (a_0, b_0). Então, sendo a_0 e a_1 as soluções da equação do segundo grau em a, por soma e produto $\left(\frac{b_0^2+k}{a_0}, b_0\right)$ é outra solução (não se preocupe, como a soma das raízes da equação é $4bk + 2b$, que é inteiro, a_1 também é inteiro; além disso, tanto a_0 como $b_0^2 + k$ são positivos). Suponha, sem perda de generalidade, que $a_0 > b_0$ (se $a_0 = b_0$, $k = 0$, logo podemos supor que um deles é maior), e suponha que a soma $a_0 + b_0$ é mínima. Então
$$\frac{b_0^2 + k}{a_0} \ge a_0 \iff k \ge a_0^2 - b_0^2 \iff \frac{(a_0 - b_0)^2}{4a_0b_0 - 1} \ge a_0^2 - b_0^2 \iff \frac{a_0 - b_0}{4a_0b_0 - 1} \ge a_0 + b_0,$$
que é um absurdo, pois
$$\frac{a_0 - b_0}{4a_0b_0 - 1} < a_0 - b_0 < a_0 + b_0.$$

Logo $a = b$. Note que $a = b$ também é suficiente, e portanto sabemos todos os pares ordenados (a, b) tais que $4ab - 1$ divide $(4a^2 - 1)^2$.

3 Expoentes

- **Diminuindo expoentes**: se $a^x \equiv 1 \pmod{m}$ e $a^y \equiv 1 \pmod{m}$ então $a^{\text{mdc}(x,y)} \equiv 1 \pmod{m}$. Isso é uma consequência direta do teorema de Bézout. Outro jeito de expressar essa propriedade é $\text{mdc}(a^x - 1, a^y - 1) = a^{\text{mdc}(x,y)} - 1$.
- **Teorema de Fermat**: $a^p \equiv a \pmod{p}$ para p primo. Se $a \not\equiv 0 \pmod{p}$ então $a^{p-1} \equiv 1 \pmod{p}$.
- **O menor divide**: Seja $\text{ord}_m a$ o menor inteiro positivo t, se existir, tal que $a^t \equiv 1 \pmod{m}$. Então $a^x \equiv a^y \pmod{m} \iff x \equiv y \pmod{\text{ord}_m a}$. Em particular, $a^u \equiv 1 \pmod{m} \iff \text{ord}_m a \mid u$.
- **Lifting the Exponent**: Seja $v_p(n)$ o maior t tal que $p^t \mid n$, p primo. Então $v_p(a^n - b^n) = v_p(a-b) + v_p(n)$ se $v_p(a-b) > 0$, $p \nmid a, b$ e p é primo ímpar. Se $4 \mid a - b$ e a e b são ímpares então $v_2(a^n - b^n) = v_2(a-b) + v_2(n)$.

Exemplo:
Encontre todos os inteiros positivos n tais que n divide $3^n - 2^n$.

Resolução:
Seja p o menor primo que divide n. Então $p \mid 3^n - 2^n$ e $p > 3$. Além disso, pelo pequeno teorema de Fermat, $2^{p-1} \equiv 3^{p-1} \equiv 1 \pmod{p}$, de modo que $p \mid 3^{p-1} - 2^{p-1}$. Logo $p \mid 3^{\text{mdc}(p-1,n)} - 2^{\text{mdc}(p-1,n)}$. Mas se o menor divisor primo de n é p, $p - 1$ e n não podem ter fatores em comum, pois todos os fatores de $p - 1$ são menores do que p. Assim, $\text{mdc}(n, p-1) = 1$ e $p \mid 3 - 2 \iff p \mid 1$, absurdo. Logo n não tem fatores primos, ou seja, $n = 1$ é a única solução.

4 Problemas

4.1 Alguns exercícios

Comece com esses aqui. Só depois faça os da próxima secção.

1. (Rússia 2009) Os denominadores de duas frações irredutíveis são 600 e 700. Encontre o menor valor possível do denominador da soma das duas frações.
2. (Rússia 2005) Encontre o menor inteiro positivo que não pode ser escrito na forma $\frac{2^a - 2^b}{2^c - 2^d}$.
3. Encontre todos os inteiros positivos a, b tais que ab divide $(a+1)(b+1)$.
4. (Rússia 2001) Sejam a, b dois inteiros positivos distintos tais que $a^2 + ab + b^2$ divide $ab(a+b)$. Prove que $|a - b| > \sqrt[3]{ab}$.
5. (APMO 2002) Encontre todos os pares de inteiros positivos (m, n) tais que $m^2 - n$ divide $m + n^2$ e $n^2 - m$ divide $m^2 + n$.
6. (Cone Sul 2006) Encontrar todos os inteiros positivos n tais que $\lfloor \sqrt{n} \rfloor - 2$ divide $n - 4$ e $\lfloor \sqrt{n} \rfloor + 2$ divide $n + 4$.
7. (Rússia 2014) Um número inteiro positivo n é *feijoada*[1] se, para todo divisor a de n, $a + 1$ divide $n + 1$. Encontre todos os números feijoada.
8. (IMO 2005) Determine todos os inteiros positivos relativamente primos com todos os termos da sequência infinita $a_n = 2^n + 3^n + 6^n - 1$, $n \geq 1$.

[1] Eu posso ter mudado alguns nomes.

4.2 Alguns problemas

1. (Finlândia 2001) Encontre todos os inteiros positivos n tais que $n^2 + 2$ divide $2001n + 2$.

2. (IMO 1994) Encontre todos os pares de inteiros positivos (m, n) tais que $mn - 1$ divide $m^3 + 1$.

3. (IMO 1998) Determine todos os pares (a, b) de inteiros positivos tais que ab^2+b+7 divide a^2b+a+b.

4. (IMO 1991) Sejam n um número inteiro maior do que 6 e $a_1, a_2, \ldots, a_k$ todos os números naturais menores do que n e primos com n. Se
$$a_2 - a_1 = a_3 - a_2 = \cdots = a_k - a_{k-1} > 0,$$
demonstre que n é primo ou n é uma potência de 2.

5. (IMO 2002) Seja $n > 1$ inteiro. Sejam $d_1, d_2, \ldots, d_k$ os divisores de n, com
$$1 = d_1 < d_2 < \ldots < d_k = n.$$
Seja $D = d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k$.
   (a) Prove que $D < n^2$.
   (b) Encontre todos os valores de n tais que D divide n^2.

6. (Ibero 2008) Prove que a equação $x^{2008} + 2008! = 21^y$ não tem soluções inteiras positivas.

7. (IMO 1988) Sejam a e b números inteiros positivos tais que $ab + 1$ divide $a^2 + b^2$. Prove que
$$\frac{a^2 + b^2}{ab + 1}$$
é um quadrado perfeito.

8. (APMO 2012) Encontre todos os pares (p, n) com p primo e n inteiro positivo para os quais $\frac{n^p+1}{p^n+1}$ é inteiro.

9. (Rússia 2012) Existe números inteiros a, b, c, todos maiores do que 10^{10}, tais que seu produto é divisível por cada um dos números mais 2012?

10. (Rússia 2009) Considere inteiros positivos $n > 1$ e $a > n^2$. Sabe-se que cada um dos números $n^2 + 1, n^2 + 2, \ldots, n^2 + n$ tem um múltiplo entre os números $a + 1, a + 2, \ldots, a + n$. Prove que $a > n^4 - n^3$.

11. (Rússia 2001) Encontre todos os inteiros positivos que podem ser representados unicamente na forma
$$\frac{x^2 + y}{xy + 1}$$
em que x e y são inteiros positivos.

12. (China 2005) Encontre todos os inteiros não negativos x, y, z, w tais que $2^x3^y - 5^z7^w = 1$.

13. (EUA TST 2009) Encontre todos os pares de inteiros positivos (m, n) tais que $mn - 1$ divide $(n^2 - n + 1)^2$.

14. Sendo $k \geq 2$ e $n_1, n_2, \ldots, n_k \geq 1$ números naturais tais que $n_2 \mid 2^{n_1} - 1$, $n_3 \mid 2^{n_2} - 1$, $\ldots$, $n_k \mid 2^{n_{k-1}} - 1$ e $n_1 \mid 2^{n_k} - 1$. Mostre que $n_1 = n_2 = \cdots = n_k = 1$.

15. (IMO Shortlist) Determine todas as ternas de números inteiros positivos $(a; m; n)$ tais que $a^m + 1$ divide $(a + 1)^n$.

16. (IMO Shortlist) Prove que, para todo inteiro positivo m, existe um número infinito de pares de inteiros (x, y) tais que:

    - x e y são primos entre si;
    - y divide $x^2 + m$;
    - x divide $y^2 + m$.

17. (IMO 2003) Determine todos os pares de inteiros positivos (a, b) tais que

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

é um inteiro positivo.

18. (Cone Sul 2012) Demonstre que não existem inteiros positivos a, b, c, d, primos dois a dois, tais que $ab + cd$, $ac + bd$ e $ad + bc$ são divisores ímpares de

$$(a + b - c - d)(a - b + c - d)(a - b - c + d).$$

19. (APMO 1997) Encontre um inteiro positivo n, $100 \leq n \leq 1997$, tal que $\frac{2^n+2}{n}$ é inteiro.

Divisibilidade – Dicas para os exercícios e problemas

Carlos Shine

1 Problemas

1.1 Alguns exercícios

1. (Rússia 2009) Os denominadores de duas frações irredutíveis são 600 e 700. Encontre o menor valor possível do denominador da soma das duas frações.

   Dicas

   A resposta é 168. Sendo $m/600 + n/700 = (7m + 6n)/4200$, mostre que o numerador é ímpar e não pode ser múltiplo de 6 nem de 7; em seguida, encontre um exemplo com $7m + 6n = 25$.

2. (Rússia 2005) Encontre o menor inteiro positivo que não pode ser escrito na forma $\frac{2^a-2^b}{2^c-2^d}$.

   Dicas

   A resposta é 11; diminua expoentes com mdc para mostrar que o número tem que ser da forma $2^k(2^{mn} - 1)/(2^n - 1) = 2^k(2^{(m-1)n} + 2^{(m-2)n} + \cdots + 2^n + 1)$, e esse número entre parênteses é, na maioria dos casos, bem maior do que 11.

3. Encontre todos os inteiros positivos a, b tais que ab divide $(a + 1)(b + 1)$.

   Dicas

   As respostas são $(1, 1)$, $(1, 2)$, $(2, 1)$, $(2, 3)$, $(3, 2)$. Repita as ideias do primeiro exemplo: mostre que $(a - 1)(b - 1) \le 2$.

4. (Rússia 2001) Sejam a, b dois inteiros positivos distintos tais que $a^2 + ab + b^2$ divide $ab(a + b)$. Prove que $|a - b| > \sqrt[3]{ab}$.

   Dicas

   Seja $d = \text{mdc}(a, b)$, $a = dx$ e $b = dy$, $\text{mdc}(x, y) = 1$. Então $x^2 + xy + y^2 \mid dxy(x + y)$. Verifique que $\text{mdc}(x, x^2 + xy + y^2) = \text{mdc}(y, x^2 + xy + y^2) = \text{mdc}(x^2 + xy + y^2) = 1$ (para esse último, eleve $x + y$ ao quadrado), de modo que $x^2 + xy + y^2 \mid d \iff a^2 + ab + b^2 \mid d^3$. Para terminar, note que $d \le |a - b|$ e $a^2 + ab + b^2 > ab$.

5. (APMO 2002) Encontre todos os pares de inteiros positivos (m, n) tais que $m^2 - n$ divide $m + n^2$ e $n^2 - m$ divide $m^2 + n$.

   Dicas

   Sendo tudo simétrico, suponha que $m \ge n$ e defina $k = m - n \ge 0$. $m^2 - n$ deve ser maior do que $m + n^2$ na maioria dos casos, e isso deve limitar k. De fato, $(n + k)^2 - n \le n + k + n^2 \iff k^2 + 2kn \le 2n + k \iff k \le 1$. Com isso, basta resolver o problema para $k = 0$ e para $k = 1$. As respostas são $(2, 2)$, $(3, 3)$, $(1, 2)$, $(2, 1)$, $(2, 3)$, $(3, 2)$.

6. (Cone Sul 2006) Encontrar todos os inteiros positivos n tais que $\lfloor\sqrt{n}\rfloor - 2$ divide $n - 4$ e $\lfloor\sqrt{n}\rfloor + 2$ divide $n + 4$.

Dicas

As respostas são 2, 36 e $q^2 + 2q - 4$, q inteiro, $q \geq 2$. Parece que é uma variável só, mas são duas: sendo $q = \lfloor \sqrt{n} \rfloor$, $n = q^2 + r$, $0 \leq r \leq 2q$ (o $2q$ é para não pular para o próximo quadrado). Com isso, $q-2 \mid q^2+r-4 \iff q-2 \mid r$ (veja que $q \equiv 2 \pmod{q-2}$) e $q+2 \mid q^2+r+4 \iff q+2 \mid r+8$. Faça os casos $q = 1$ e $q = 2$ separadamente e estime $k = (r+8)/(q+2)$ (resposta: $k \leq 2$). Aí basta substituir o k nos dois casos e fazer as contas.

7. (Rússia 2014) Um número inteiro positivo n é *feijoada*[1] se, para todo divisor a de n, $a + 1$ divide $n + 1$. Encontre todos os números feijoada.

   Dicas

   A resposta é 1 e os primos ímpares. Se $n = 1$ ou é primo ímpar é imediato que dá certo. Se não, escreva $n = ab$, $a \geq b \geq 2$, e chegue a um absurdo usando a desigualdade divisor $\leq$ múltiplo. O caso que falta, $n = 2$, também é imediato.

8. (IMO 2005) Determine todos os inteiros positivos relativamente primos com todos os termos da sequência infinita $a_n = 2^n + 3^n + 6^n - 1$, $n \geq 1$.

   Dicas

   A resposta é só 1. Basta ver os primos; fazendo casos pequenos para $p \geq 5$ vemos que a_{p-2} é múltiplo de p. Aplique pequeno Fermat para ver que dá certo e faça os casos $p = 2$, $p = 3$ separadamente.

1.2 Alguns problemas

1. (Finlândia 2001) Encontre todos os inteiros positivos n tais que $n^2 + 2$ divide $2001n + 2$.

   Dicas

   As respostas são 6, 9 e 2001. Mostre que $n \leq 2001$ e obtenha, com combinações lineares ou congruências, $n^2 + 2 \mid 2 \cdot 2001^2 + 4$. Fatore $2 \cdot 2001^2 + 4 = 8008006 = 2 \cdot 19 \cdot 83 \cdot 2539$. Agora, $n^2 + 2$ é congruente a 2 ou 3 módulo 4, e isso elimina um bocado de casos (separe em n par e n ímpar).

2. (IMO 1993) Encontre todos os pares de inteiros positivos (m, n) tais que $mn - 1$ divide $m^3 + 1$.

   Dicas

   Com combinações lineares, prove que $mn - 1 \mid n^3 + 1$ também, o que nos dá a simetria que permite supor que $m \geq n$. Prove também que $mn - 1 \mid m + n^2$ e faça $m = n + k$, $k \geq 0$. Limite k (é no máximo 3) e substitua os quatro casos. As respostas são $(2, 2)$, $(1, 2)$, $(2, 1)$, $(1, 3)$, $(3, 1)$, $(3, 5)$, $(5, 3)$, $(2, 5)$, $(5, 2)$.

3. (IMO 1998) Determine todos os pares (a, b) de inteiros positivos tais que ab^2+b+7 divide a^2b+a+b.

   Dicas

   Use combinação linear para diminuir o grau e achar que $ab^2 + b + 7 \mid b^2 - 7a$. Se $b^2 = 7a$, obtemos $(7k^2, 7k)$ que é solução (não se esqueça de testar!). Se não, $ab^2 + b + 7 \leq |b^2 - 7a|$; se $b^2 - 7a > 0$, não dá porque $ab^2 + b + 7 > b^2 > b^2 - 7a$; se $b^2 - 7a < 0$, $b \leq 2$ (por quê?), e é só testar $b = 1$ e $b = 2$. As respostas são $(7k^2, 7k)$, $(11, 1)$ e $(49, 1)$.

4. (IMO 1991) Sejam n um número inteiro maior do que 6 e $a_1, a_2, \ldots, a_k$ todos os números naturais menores do que n e primos com n. Se

   $$a_2 - a_1 = a_3 - a_2 = \cdots = a_k - a_{k-1} > 0,$$

   demonstre que n é primo ou n é uma potência de 2.

[1] Eu posso ter mudado alguns nomes.

Dicas

Pense em $a_2 = p$ primo. Se $p = 2$ ou $p = 3$ o problema essencialmente acaba, então n é múltiplo de 6. Seja $r = a_{i+1} - a_i = p - 1$. Observando a_k, prove que $p - 1 \mid n - 1$. Considere um primo $q \mid p - 1$. Note que $q < p$, então $q \mid n$, e lembrando que $q \mid n$, $q = 2$, ou seja, $p = 2^m + 1$. Mas aí $a_3 = 2p - 1 = 2^{m+1} + 1$, e um dos expoentes m, $m + 1$ é ímpar, que dá absurdo.

5. (IMO 2002) Seja $n > 1$ inteiro. Sejam $d_1, d_2, \ldots, d_k$ os divisores de n, com

$$1 = d_1 < d_2 < \ldots < d_k = n.$$

Seja $D = d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k$.

   (a) Prove que $D < n^2$.

   (b) Encontre todos os valores de n tais que D divide n^2.

Dicas

Para o item a, note que $d_i = n/d_{k+1-i}$, e mostre que a soma dos inversos de d_id_{i+1} é menor do que 1 (faça uma estimativa bem tosca, como $d_i \geq i$, e telescope). Para o item b, cuja resposta é n primo, considere o menor divisor primo $d_2 = p$ de n e veja que se n não é primo $D > n^2/d_2 = n^2/p$ e se $D \mid n^2$, $D \leq n^2/p$, dando absurdo.

6. (Ibero 2008) Prove que a equação $x^{2008} + 2008! = 21^y$ não tem soluções inteiras positivas.

Dicas

x é múltiplo de 21 implica $21^y > 21 \iff y > 2008$ implica $21^{2008} \mid 2008!$, que é absurdo.

7. (IMO 1988) Sejam a e b números inteiros positivos tais que $ab + 1$ divide $a^2 + b^2$. Prove que

$$\frac{a^2 + b^2}{ab + 1}$$

é um quadrado perfeito.

Dicas

Seja $k = (a^2 + b^2)/(ab + 1)$ e estenda os pares (a, b) para não negativos. Suponha que (a_0, b_0) tem $a_0 \leq b_0$ e $a_0 + b_0$ mínimo e mostre que $a_0 = 0$, usando a equação $x^2 - kax + a^2 - k = 0$. Veja que $(a_0, ka_0 - b_0)$ também é solução, logo $ka_0 - b_0 \geq b_0$. Com isso, $a_0(a_0^2 + b_0^2) \geq 2b_0(a_0b_0 + 1) \iff a_0^2 \geq a_0b_0^2 + 2b_0$, que dá errado se $a_0 > 0$. Pode ocorrer de $ka_0 - b_0$ (veja o produto das raízes) ser negativo, ou seja, $ka_0 - b_0 \leq -1 \iff a_0(a_0^2 + b_0^2) \leq (b_0 - 1)(a_0b_0 + 1)$, que você pode verificar que dá errado também.

8. (APMO 2012) Encontre todos os pares (p, n) com p primo e n inteiro positivo para os quais $\frac{n^p+1}{p^n+1}$ é inteiro.

Dicas

Fixe p. Se $p > 2$, $p^n + 1 > n^p + 1$ para $n > p$ (basta ver que $p^n/n^p = (p^{n/2p}/\sqrt{n})^{2p}$ e $p^{n/2p} = (1 + p - 1)^{n/2p} > 1 + (p - 1)n/2p = 1 + n/2 - n/2p > \sqrt{n}$ para $n \geq 4$ e $p \geq 3$. Assim, $n \leq p$. p é ímpar, então $p^n + 1$ é par e n é ímpar, e dá para fatorar $p^n + 1$ com $p + 1$ como um de seus fatores, e $p + 1 \mid n^p + 1$. Veja que $p^p \equiv n^p \pmod{p + 1}$ e $\phi(p + 1) < p$, logo $n \equiv p \pmod{p + 1}$ e $n = p$. Para $p = 2$, limite n para 4 e teste os casos. As respostas são (p, p), p primo, e $(2, 4)$.

9. (Rússia 2012) Existe números inteiros a, b, c, todos maiores do que 10^{10}, tais que seu produto é divisível por cada um dos números mais 2012?

Dicas

Temos muitas possibilidades, então é de se esperar que a resposta seja sim. Troque 10^{10} por M e 2012 por n. Sejam $x = a + n$, $y = b + n$ e $z = c + n$; queremos $x \mid (x - n)(y - n)(z - n) \iff x \mid n(y - n)(z - n)$. Faça então $x = kn$, $y = \ell n$ e $z = mn$; temos $k \mid n^2(\ell - 1)(m - 1)$ e análogos. Que tal $k = \ell - 1$? Temos $\ell \mid n^2(\ell - 2)(m - 1)$ e $m \mid n^2(\ell - 1)(\ell - 2)$. Podemos fazer $m = (\ell - 1)(\ell - 2)$ e $\ell = 2n^2$. Aí $a = (2n^2 - 2)n$, $b = (2n^2 - 1)n$ e $c = (2n^2 - 1)(2n^2 - 2)n - n$. Basta ver se $2(2012^2 - 1)2012 > 10^{10}$, o que é verdade.

10. (Rússia 2009) Considere inteiros positivos $n > 1$ e $a > n^2$. Sabe-se que cada um dos números $n^2 + 1, n^2 + 2, \ldots, n^2 + n$ tem um múltiplo entre os números $a + 1, a + 2, \ldots, a + n$. Prove que $a > n^4 - n^3$.

    Dicas

    Note que a diferença entre dois números entre $a+1$ e $a+n$ é no máximo $n-1$, então cada número n^2+k tem no máximo um divisor nesse intervalo; ou seja, é um de cada. Considere o divisor n^2+k de $a + n$. Se $k < n$, um número $a + i = m(n^2 + k + 1)$, e vendo módulo $n^2 + k$ temos $m \equiv -n + i \pmod{n^2 + k}$. Ou seja, $m \geq n^2 + k - n + i > n^2 - n$ e $a + i > (n^2 - n)(n^2 + k + 1) > n^4 - n^3$. Se $k = n$, tome o divisor de $n^2 + k$ de $a + n - 1$.

11. (Rússia 2001) Encontre todos os inteiros positivos que podem ser representados unicamente na forma
$$\frac{x^2 + y}{xy + 1}$$
em que x e y são inteiros positivos.

    Dicas

    A resposta é todos os inteiros maiores do que 1. Para $y = x+1$ obtemos 1, e não é único. Também é possível qualquer inteiro tomando $x = y^2$. Um jeito de ver isso é notar que $xy + 1 \mid x - y^2$ com combinação linear. Com isso, se $x \neq y^2$ então $xy + 1 \leq |x - y^2|$ e, do original, $xy + 1 \leq x^2 + y$. Se $|x - y^2| = x - y^2$, não dá certo (o divisor é maior); se $|x - y^2| = y^2 - x$, temos $xy + 1 \leq y^2 - x \iff x \leq y - 1$. Além disso, $xy + 1 \leq x^2 + y \iff y \leq x + 1$. Logo $y = x + 1$ e nesse caso a fração é igual a 1. Note que encontramos todas as soluções.

12. (China 2005) Encontre todos os inteiros não negativos x, y, z, w tais que $2^x 3^y - 5^z 7^w = 1$.

    Dicas

    Se todas as variáveis são positivas, veja módulo 7 e sendo $3^2 \equiv 2 \pmod 7$, prove que y é par; vendo módulo 5, prove que x é par; e veja módulo 3 para achar a paridade de z (vou deixar você descobrir qual é). Com isso, fatore, tire mdc, e use LTE.

    Se um deles é zero, não é x; todos menos x podem ser zero, e obtemos $(1, 0, 0, 0)$. Se $y = 0$, veja módulo 4. Mostre que x é múltiplo de 3, e fatore de novo. Se $y > 0$, veja módulo 3, e mostre que $z > 0$, e portanto $w = 0$, e caímos no caso anterior.

    As soluções são $(2, 2, 1, 1)$, $(1, 0, 0, 0)$, $(3, 0, 0, 1)$ e $(1, 1, 1, 0)$.

13. (EUA TST 2009) Encontre todos os pares de inteiros positivos (m, n) tais que $mn - 1$ divide $(n^2 - n + 1)^2$.

    Dicas

    A resposta é $(2, 2)$, $(t^2 + 1, (t + 1)^2 + 1)$ e $((t + 1)^2 + 1, t^2 + 1)$, t inteiro não negativo. Primeiro prove que $mn - 1$ também divide $(m^2 - m + 1)^2$ para ganhar simetria. Depois diminua o grau: $mn-1 \mid (m+n-1)^2$. Depois considere a solução mínima (m_0, n_0), com $m_0 \leq n_0$ e m_0+n_0 mínimo, e seja $k = (m+n-1)^2/(mn-1)$, e obtemos a equação $x^2 - (km_0 - 2m_0 + 2)x + (m_0 - 1)^2 + k = 0$. Então $(m_0, ((m_0-1)^2+k)/n_0)$ é também solução. Logo $(m_0-1)^2+k \geq m_0 n_0 \iff (m_0+n_0-1)^2 \geq$

$(m_0n_0-1)(m_0n_0-(m_0-1)^2) \iff n_0+m_0^2 \geq m_0^2n_0+2m_0 \iff n_0(m_0^2-1) \leq (m_0-1)^2-1 < m_0-1)^2 \implies n_0 < m_0+1$ ou $m_0=1$. Ou seja, $m_0=n_0$ ou $m_0=1$.

Se $m_0=n_0$ então $m_0^2-1 \mid (2m_0-1)^2 \iff m_0^2-1 \mid 4m_0+5 \implies m_0^2-1 \mid 9$, e temos $m_0=2$; de fato, a única solução com $m=n$ é $(2,2)$.

Se $m_0=1$, $n_0-1 \mid n_0^2 \implies n_0=2$, que dá certo, e $k=(1+2-1)^2/(1\cdot 2-1)=4$. Nesse caso, cada nova solução é obtida trocando n por $4m-2m+2-n=2m+2-n$, e obtemos a recursão $a_0=1$, $a_1=2$ e $a_{m+1}=2a_m+2-a_{m-1}$. Vendo alguns casos pequenos: $1,2,5,10,17$. Parece que $a_m=m^2+1$, o que é fácil de provar por indução. Com isso, podemos achar todas as soluções.

14. Sendo $k \geq 2$ e $n_1,n_2,\ldots,n_k \geq 1$ números naturais tais que $n_2 \mid 2^{n_1}-1$, $n_3 \mid 2^{n_2}-1$, $\ldots$, $n_k \mid 2^{n_{k-1}}-1$ e $n_1 \mid 2^{n_k}-1$. Mostre que $n_1=n_2=\cdots=n_k=1$.

    Dicas

    Seja $M=\text{mmc}(n_1,n_2,\ldots,n_k)$. Prove que $M \mid 2^M-1$ e mostre que $M=1$ usando as mesmas ideias do exemplo 3.

15. (IMO Shortlist) Determine todas as ternas de números inteiros positivos $(a;m;n)$ tais que a^m+1 divide $(a+1)^n$.

    Dicas

    Verifique que m é ímpar ou $a=1$ ($(1,m,n)$ é solução). Se $m>1$ ($(a,1,n)$ é solução), use LTE para mostrar que $(a^m+1)/(a+1) \mid m$ e faça uma desigualdade para mostrar que $a \leq 2$ e $m \leq 3$. Com isso, a outra solução é $(2,3,n)$, $n \geq 2$.

16. (IMO Shortlist) Prove que, para todo inteiro positivo m, existe um número infinito de pares de inteiros (x,y) tais que:

    - x e y são primos entre si;
    - y divide x^2+m;
    - x divide y^2+m.

    Dicas

    Veja que $xy \mid x^2+y^2+m$ e se $k=(x^2+y^2+m)/xy$ dá para construir infinitos pares usando equação do segundo grau (como no exemplo 2). É possível até achar todas as possibilidades!

17. (IMO 2003) Determine todos os pares de inteiros positivos (a,b) tais que

$$\frac{a^2}{2ab^2-b^3+1}$$

    é um inteiro positivo.

    Dicas

    As soluções são $(2n,1)$, $(n,2n)$ e $(8n^4-n,2n)$, n inteiro positivo. Note que $2a-b \geq 0$. se $b=2a$ dá certo, então seja $k=2a-b>0$. Substitua e reduza a $4(kb^2+1) \mid (b+k)^2$. Separe $b=1$ (substitua direto com a). Faça a desigualdade para obter $k \geq 4b^2-2b$. Combinação linear leva a $4(kb^2+1) \mid b^4-2b-k$. $k=b^4-2b$ nos dá a outra família infinita de soluções. Se não, a desigualdade nos dá $k \leq b^2-2$, que é um absurdo com a outra desigualdade. (As contas não saem tão simples assim; é preciso fazer algumas estimativas.)

18. (Cone Sul 2012) Demonstre que não existem inteiros positivos a,b,c,d, primos dois a dois, tais que $ab+cd$, $ac+bd$ e $ad+bc$ são divisores ímpares de

$$(a+b-c-d)(a-b+c-d)(a-b-c+d).$$

Dicas

Primeiro mostre que $\text{mdc}(ab+cd, ac+bd) = 1$: se $p \neq 2$ divide $ab+cd$ e $ac+bd$, divide a soma $(a+d)(b+c)$ e a diferença $(a-d)(b-c)$. Se $p \mid a+d$ e $p \mid a-d$, $p \mid \text{mdc}(a,d)$; o mesmo para b e c. Se $p \mid a+d$ e $p \mid b-c$ então divide $(a+b-c-d)(a-b+c-d)(a-b-c+d) \equiv 2a \cdot 2d \cdot 2b \equiv 0 \pmod{p}$, e p divide a, b ou d, e divide d, c ou a respectivamente, absurdo de novo.

Então $(ab+cd)(ac+bd)(ad+bc) \mid (a+b-c-d)(a-b+c-d)(a-b-c+d)$ e fazemos a desigualdade para ver que dá errado; o único caso que sobra é $a+b = c+d$ e análogos, mas veja paridade para ver que um deles é par e os outros são ímpares.

19. (APMO 1997) Encontre um inteiro positivo n, $100 \leq n \leq 1997$, tal que $\frac{2^n+2}{n}$ é inteiro.

Dicas

Tente encontrar $n = 2pq$, p, q primos ímpares distintos. Devemos ter $2^{2pq-1}+1 \equiv 0 \pmod{p} \iff 2^{2q-1} \equiv -1 \pmod{p}$. Veja que $(2^{(p-1)/2})^2 \equiv 1 \pmod{p} \iff 2^{(p-1)/2} \equiv \pm 1 \pmod{p}$. Se $2^{(p-1)/2} \equiv -1 \pmod{p}$, podemos tentar $2q-1 = (p-1)/2 \iff p = 4q-1$. Analogamente, $2^{2p-1} \equiv -1 \pmod{q} \iff 2^{8q-3} \equiv -1 \pmod{q} \iff 2^5 \equiv -1 \pmod{q} \iff q = 3$ ou $q = 11$. No primeiro caso, $p = 11$ e $n = 66$; no segundo caso, $p = 43$ e $n = 946$. De fato, uma busca no computador mostra que $n = 946$ é a única possibilidade.